A Study on Mapping Internet Exchange Points based on their Peering Matrixes and Shed Lights

Dr. Najumul Saqib and Imran Sajid Shahid

Abstract--- *Internet Exchange Points (IXPs) considerably take part an imperative responsibility in the Internet AS level ecosystem exchanging 20% of the overall internet inter-domain traffic. At present, there are approximately 40,000 ASes. Even though IXPs contribution in the internet traffic is increasing gradually, extremely modest effort is made for discovery of peering matrixes in the IXPs i.e. peering of ASes inside an IXP and the reasons of peering. Here, IXP properties are studied based on their peering matrixes and shed lights on few schemes by which peering among members in IXP can be detected and effectively verified. This comprises the openly available datasets which can be utilized for finding such peerings and can also infer ASes that take part in IXPs. There are around 58k peering links which are identified by using several schemes and discussed IXP properties in accordance to their size, geographical location etc. finally, summarized that there is a considerable deviation among publicly available datasets and the one utilized for finding IXP mapping. This can be effectively improved by using different techniques and can have a better impact on understanding IXP characteristics.*

Keywords--- *Internet Exchange Point, Peering, Internet Service Provider.*

I. INTRODUCTION

THE Internet is a huge collection of Autonomous Systems (ASes) dispersed all over the world and interconnected with each other. These Autonomous Systems belongs to various Internet Service Provider Companies (ISPs), Content Providers, Webhosters, Universities and other enterprises. Each Autonomous System has its own local policies and based on those policies ASes import and export routes from their neighbors. Beyond the evolution of Internet Protocol, there has been a significant change in the Internet topology which impacts the AS relationships and also there peering policies. For understanding the current state, it is of utmost importance to understand and infer factors that involves in making these dynamics. Taking a single snapshot of the internet eco-level system for evaluating any algorithm/protocol would not be appropriate, as the data on which the results are based might becomes outdated by the time the desired algorithm/protocol is going to be implemented. Thus, better network planning and designing requires a greater understanding of the Internet AS level topology. The setting up of Internet Exchange Points (IXPs) is beneficial from economic perspective for ASes to

peer directly with other ASes at IXPs [1]. Increase in the peering at Internet Exchange Points have led researchers to work more in this field as a lot of peering links is still uncovered which might impacts our understanding of the internet AS level topology [2]. Still, with all the significant efforts has been made so far, Internet AS level topology has remained an open challenge because of shortcoming of the available measurements methods. Most commonly used techniques includes traceroute based data, BGP table dumps driven data and searching relevant data in Internet Routing Registries (IRR). Though, studying the nature of the internet AS level topology is a complex task, as the data required for such studies is hard to find by and with questionable accuracy. Recent studies agree on the fact that by using the publicly available datasets, we can infer the number of Autonomous Systems and also their peerings. But they all conclude that even by using all these available measurements tools and data sets, around 35% to 95% of inferred AS maps still misses the peer-to-peer relationship which cannot be neglected [2, 3, 4].

A. IXPs Background

Internet exchange points (IXPs) facilitates around 20% of the total internet inter-domain traffic. If we draw a graph of the internet and consider nodes as an Autonomous Systems, then two nodes connecting each other reflects a business relationship for exchanging data traffic. Connectivity of Autonomous Systems with each other can be made through dedicated/private links (point-to-point) or through public Internet Exchange Points. Advantages of private peering is that we have dedicated bandwidth, easier troubleshooting but at a high cost.

With the recent trend towards public peering at Internet Exchange Points; ISPs and other companies are migrating to be a part of IXP because of the significant benefits like an AS can peer with any other member within that IXP by agreeing on some settlement. It saves the infrastructural cost that every party has to bear in case of private peering. Benefit for ISPs is that, there is no hassle of maintaining that public peering link in an IXP as IXPs are usually managed by third parties with some fees taken by every member on monthly or annual basis.

Members in an IXP exchange their reach ability information through Border Gateway Protocol (BGP) which is an inter-domain reachability protocol that allows ASes to apply their own policies according their business relationships and select/propagates routes accordingly.

If an AS is physically connected at an IXP; that does not mean an AS can interact with every other AS in that IXP [5]. ASes inside an IXP first has to make contractual agreements for the exchange of traffic between them. These relationships include customer-provider, peer-to-peer and backup. In

Dr. Najumul Saqib, Imperial College London, UK.

Imran Sajid Shahid, Heavy Industry Taxila Education City University, Pakistan.

DOI : 10.9756/BIJEMS.8321

customer-provider relationship, customer pays its provider and provider assures customer for global reachability. In *peer-to-peer* relationship, peers exchange data traffic of their customers for free or with very low cost. It is also known as “settlement-free-interconnection”. Peering is one of the most effective methods for Internet Service Providers in order to cut down the transit cost.

Figure 1, shows a simple IXP architecture where four Autonomous Systems are participating in the IXP. If AS1 wants to have a peering with any of the other AS in the IXP, first they need to agree and define a peering policy of this connection. Then they have to establish a BGP peering session for communication and start exchange data traffic. Internet Exchange Points provide infrastructure where multiple ISPs connect with each other subject to their business objectives. For ISPs, peering at the IXP become much simpler because IXP already have the required physical infrastructure for peering connectivity so ISP can peer with any other ISP within a single platform. By bypassing their transit providers, ISPs not only cut down their traffic costs but also have better Quality of Service (QoS) of data exchange between their peers [6].

Figure 1: A Sample IXP

The size of the Internet Exchange Point varies from few members sharing data traffic for several *Mbps* to few hundred members exchanging more than 1 *Tbps* of traffic [8]. Many Internet Exchange Points publish their information on the website and some other internet routing repositories for attracting more customers and some IXPs did not publish it openly. Usually, this published information includes peering of the members in that particular IXP, their traffic statistics and port capacities. From the last few years, discovering those low-tier peering links and their traffic matrixes has been an active area of research [2, 9]. Current statistics shows that there are more than 200 operational IXPs worldwide, which shares around 6-7 *Tbps* of two way traffic which is 15-20% of the total internet inter-domain traffic [7]. Usually, the internet data traffic depends on the number of peering members in an IXP and below is a snapshot of SIX IXP whose total data traffic ranges from 15-35 Gbps.

This paper discuss the IXP characteristics and approaches by which IXP related data can be collected from different resources, which helps for a better understanding of those peering matrices in IXPs (i.e. who peers with whom at which IXP) [12]. Although, IXPs play a vital role in the AS level topology construction, the properties of IXPs such as geographical location, size distributions and members in an IXP makes a large impact on AS topology.

Rest of the paper is structured as follows: Sec. 2 discusses the conventional IXP architecture. Sec. 3 describes the key ingredients of collecting data from various resources and other methods by which data can be collected and inferred. Sec.4 presents the IXP characteristic and analysis. The paper is summarized with some of the lessons we learned from our approach in Sec. 5.

Figure 2: SIX IXP Member's Data Traffic

B. Related Work

Research community focus on finding the AS level topology information is significant and emphasizing on the empirical observations. AS level topology modeling relied on the large scale traceroute experiments and BGP table data that inferred different properties and peerings between Autonomous Systems. However, there is an increasing evidence that the data collected and inferred from BGP table data and traceroute experiments is of insufficient proof and difficult to refer the complete AS level topology [10, 11]. [12] work highlighted the inadequacy in the approach of finding the AS level topology and presented few methods for inferring peering. They also shed some lights on the need for better alternative approaches for modeling AS level topology.

Many IXPs as a business strategy or for attracting customers publish a lot of useful information such as their location, members, daily traffic and also the fees structure. There are two projects which systematically gather all this information and make a database which is publicly available. They are Packet Clearing House (PCH) and PeeringDB (PDB) [12]. Since, IXPs treat their peering arrangement as a personal propriety and sometimes are not willing to publish their records; accuracy of the information on the websites is still a challenging debate. Indeed, hundreds of IXPs are deployed around the world and attracting customers by claiming high QoS, low latency and low cost; properly studying its dynamics may reveal a lot of useful information for mapping a better AS level peering.

II. CONVENTIONAL IXP ARCHITECTURE

A typical IXP architecture requires a physical infrastructure where different Autonomous System can plug in their access routers and connect with other members in that IXP. Fig. 3, shows a very simple IXP architecture. In this figure, an IXP is having six members and all members are represented by their AS numbers. When two members in this particular IXP wants to peer with each other, first they have to start a BGP session and then traffic can flow based on their policies. One thing which is noticeable over here is that IXP

will assign an IP address to every member participating in the IXP. All the IXPs in the world get a separate IP address block by Internet Registry responsible for those IXPs which they further distribute it to their members [12]. For example in fig. 2, IXP has an IP address block of 195.69.144.0/22, the IXP facing router interface of AS1 as assigned by IXP is 195.69.144.1 and very similarly for AS4 is 195.69.144.4.

The basic approach to identify an IXP is through traceroute tool. This can also help in finding the peering among IXP members and we can infer peering properties that if there is an IXP prefix in the traceroute path. The key to this approach is that [12, 13] we must know the IXP prefixes. In Fig. 2, by running a traceroute probe within any source from AS1 to AS4, the packet traverses through different networks to reach destination. If the sequence in the traceroute appeared as: AS1, 195.69.144.4 and AS4, and we already know the IXP prefix of AS4, it leads to know us that the trace must have gone through this IXP because the IP prefix 195.69.144.0/22 belong to this IXP.

Figure 3: Typical IXP Architecture with 6 ASes (Members)

We also made another assumption that this will only occur if all the routers respond to the traceroute request otherwise results would be different and lead towards wrong inference. This technique tells us that AS1 and AS4 are part of this IXP and also peering each other. The problem which might occur by this method is that there are various ASes that has private AS numbers, so finding their IXP assigned address is a difficult work.

III. DATA SOURCES

AS level eco-system is decentralized and widely spread geographically. To have a single repository from where accurate data can be extracted is very difficult. Researchers are trying to apply different techniques from multiple resources to get IXP specific data of varying quality.

A. IXPs Website and Databases

IXP related information can be collected by visiting website of the IXPs. IXPs usually put technical and non-technical data on their web such as their daily traffic, location and members etc. One of the reasons would be to attract more business and members by publishing all their information. But accuracy of this data in order to infer proper peering is still a

question mark [13]. Although, not all IXPs publish their information on the web, we cannot only rely on the websites to infer such properties.

Two very rich sources of getting IXP related information at a centralized place are Packet Clearing House (PCH) [14] and PeeringDB (PDB) [15]. Information available on these projects is IXP geographic location, Prefix, list of the IXP members and links to their website if there is any [12]. They also provide some statistical analysis like top 10 Exchange Points in terms of data traffic, or top 10 countries having highest number of IXPs. Database on their web is based on voluntary contributions. PeeringDb encourages the IXPs to publish and maintain their database in PeeringDB directory.

B. Internet Routing Registry (IRR)

Internet Routing Registry is a database where network operators are encouraged to share their BGP policies in order to avoid problematic conflicts between Internet Service Providers. IRR is helpful in the sense that the import and export attributes in routing table of ISPs may indicate the presence of BGP peering routers. Again, the key to this method is to know the IXP prefixes. For example, the peering link between Linx Telecom (AS3327) and Wind Telecom (AS1267) at Amsterdam IXP (AMS-IX) is:

```
aut-num: AS3327
import: from AS1267 195.69.145.236
```

AMS-IX has IP address allocation range 195.69.144.0/22 which means it can have approximately 1k participants. This approach gives very useful information as it directly show the AS number and if we already know the IXP prefixes, it makes a lot easier to find that these ASes peers at this particular IXP.

C. Looking Glass Servers

Many Internet Service Providers run a public Looking Glass Server (LG) which can be accessed remotely for the purpose of viewing routing information. Route servers can also reveal this information but LG Server websites shows the interface from where user can run commands such as ping, traceroute or show ip bgp summary [16]. Commands varies from one looking glass server to another, as some LG server are more capable of issuing commands and some shows very few commands. *Show ip bgp summary* command is most useful for finding the peering. Unfortunately, we cannot rely totally on this method as if the Looking server is located outside an IXP than BGP information is of no use for us. Finding LG server of an AS inside an IXP is helpful for mapping any peering.

D. BGP Tables

BGP table snapshots [12] can be collected from many route servers located at many major IXPs. BGP routers that communicate directly to other routers are known as BGP speakers (neighbors). BGP speakers within each Autonomous exchange reachability information based on a set of policies in order to give a consistent image of an AS to other ASes. By issuing command such as *show ip bgp summary* will provide all the BGP sessions of that router and if routers peer at an IXP, then as discussed earlier their ip address will be the one as allocated by an IXP.

Neighbor	AS
195.69.146.247	15169

Above is an example which shows that when this command runs on a BGP router operated by Packet Clearing House (AS3856) then it shows that Google (AS15169) has a peering session with Packet Clearing House at Amsterdam Internet Exchange (AMS-IX) which has an ip address 195.69.146.247/22. This method is very useful because a single probe of bgp can infer many IXP related peering results as compared to traceroute query which will only reveal one possible result.

Many projects have also generated traceroute probes snapshots which can be used for extracting peering between ASes and also tracking IXPs. Projects such as SKITTER [17] and DIMES [18] collected all this information and their data set can be manipulated to infer different properties. By getting data from various resources lead towards more accuracy rather than just relying on a single snapshot of AS level topology.

Another basic method to check the existence and liveness of an IXP is to send *ping* commands to check whether the IXP still exist or not. Negative response leads towards two things, either the IXP blocks ICMP packets or IXP prefix is not advertised globally so it is not appearing on global BGP tables [12].

E. Targeted Source Routing

Another approach to find IXP related peering is targeted source routing. It is possible to traverse a packet according to our needs rather than router makes the decision of forwarding the packet. It is like IPv4 option Loose Source Record Route (LSRR) in which user forces a packet to traverse a particular router before reaching the destination. Very similarly, [24] use this approach with traceroute to traverse a particular pair of IXP members. If there are two Autonomous System AS1 and AS2, first we need to identify LSSR capable router in AS1 so we can traverse our traceroute probe to first go through AS1 before reaching AS2. If the packet goes through AS1 to AS2, it will show the IXP assigned address which leads to conclusion that AS1 and AS2 peers at this IXP. But the known problem with LSSR is that it is being blocked by many network operators as a threat to their security infrastructure [23]. Still, for verifying any particular IXP related peering, this approach can be used for matching the accuracy.

IV. IXP CHARACTERISTICS AND ANALYSIS

There are more than 200 IXPs [12] active at the moment. Packet Clearing House report shows that 91 countries have at least one IXP and 107 countries still do not have this facility [14]. Majority of this IXP trend is found in European Countries [15] which confirms that IXPs are more prevalent method of interconnection in Europe rather than other countries [13]. There are around 2300 looking glass servers in around 66 countries from where we can run simple commands for querying data. Study also shows that there are around 58000 IXP related peering at IXPs. DIMES statistics shows that there are 155 IXPs with 17.5 k peerings and CAIDA database shows 102 IXPs with 2.6k peerings. Since the quality

of this data is unknown, [12] finds around 214 IXPs with 44k IXP related peerings and their validation results claimed that they have got the largest data set for finding such statistics.

Table 1: IXPs, Members and their Peerings Publicly Available [12]

Dataset	IXPs	Members	Peerings
DIMES	155	1.9k	17.5k
CAIDA	102	1k	2.6k
Planetlab	122	1.8k	8.3k

The reason why it is difficult to map any member by just relying on one data set or technique is that there is not a single tool which satisfies peering condition. Sometimes there are limitations of the method, like in targeted source routing we are totally relying on the fact that the other AS is capable of handling such ICMP request. If it is not capable, then this did not mean that this method is useless. Combination of different approaches at the end can lead towards a correct data set for mapping. Another problem is that some IXPs own different Autonomous system numbers so mapping would be different in this case [22]. For example, Verisign is having AS7342 and AS26415 at Amsterdam Exchange (AMS-IX).

Table 2: IXP Database Contributions

Database	IXPs	Members	Peerings
DNS	84	2k	0
PeeringDB	253	1k	0
PCH	332	2.2k	0
IXP websites	166	4k	3.1k
IRR	80	2k	18k

Table 2 is a summary of comparison with public IXP databases. Finding member's information of an IXP can be achieved through IXP websites or databases which store this information. There are approximately 166 IXPs which publish lists of their members. Analysis shows that DE-CIX is having 8.9k peerings and AMS-IX 8.6k [15] which is the largest number of peerings at an IXP in Europe. One thing to notice over here is that the method for finding IXP related peering as described in sec. 2, will not be applicable if two ASes have private peering, which means they have a direct connection from their router to another router bypassing the IXP fabric. If this is the case, this method will not be able to detect the peering.

Another interesting study for finding these peering is being carried out by [13]. They perform analysis on how Autonomous System interconnects at IXPs. Study shows that most of the members at IXPs are transit ASes which peer aggressively with others in order to reduce the transit cost. Stub Autonomous System usually connects to an IXP in order to have global connectivity by peering transit provider in IXP.

A. Peering Matrix

Peering matrix indicates whether two members in an IXP peers with each other or not. This property is symmetric, so the peering matrix would also be symmetric. There could be many reasons for peering in an IXP and also for not peering; but typically ASes peers with each other when both are having some financial benefit [19]. If an AS connect its router to an IXP; AS can connect with any other member in the IXP by

making some contractual agreements. IXP provides ASes the facility to peer with any other AS within a single platform. That leads towards the dynamic behavior of peering matrix in IXPs. Some IXPs publish their peering matrix on the web and other IXPs treat this information as their proprietary and did not disclose it. For example, Internet Neutral Exchange Association (INEX) publishes their member list, daily traffic and peering matrix on their website [20]. There are 87 participants in that IXP and most of them almost peer with every other participant in that IXP. By having this information, we can also classify how many content and network providers are present in this IXP and who peers with whom. The only drawback of having such information is that we need to check at several times the peering matrix because sometimes AS presents in an IXP will not appear in peering matrix because they do not want to disclose this information or maybe they are not currently peering with any other member. Peering links tends to be there unless an ISP disappeared from that IXP [21].

B. Peering Density

Major difference in terms of AS-level topology at IXP level and global AS level topology is the density of interconnections [19]. It's a very common metric used to define likelihood of peering between two members in an IXP. Basically it is the ratio between numbers of actual peering links to the number of all the possible AS pairs participating in that IXP. Larger value of peering density shows that peering links are more aggressively found in that particular IXP. As studied, the normal value of peering density of IXPs in Europe who publish their peering matrix is around 70%. The peering matrix of US based IXPs are lower than that of European based IXPs.

We cannot neglect the fact that different members in an IXP have different peering policies. PeeringDB shows the peering policy of members enrolled in an IXP and it is publicly available. Open policy of an AS means AS is willing to have peering connection with any other member either it is content provider or network. While AS having selective peering policies will tends to have lower number of peerings as compared to the one having open policy.

C. Peering in IXPs

By the methods defined in Sec.3, [21] collected around 58k peering links in all the IXPs presented till their study. Peering information can be collected from several resources as already discussed; but the validation of those links is still questionable in terms of accuracy. For example, CAIDA only have the record of 2.6k peering links and DIMES have around 17k. After associating all the 58k routes to their respective IXPs; ranking them in descending order in terms of peering is shown in fig. 4. On the x-axis, IXPs ranked by number of peerings and on y-axis actual number of peerings. [21] Ranked them in terms of low, medium and high confidence peerings.

Ranking is just to show the confidence in the results gathered by different unique approaches and from the public available datasets. High confidence means the number of peerings calculated from the approach such as LG servers, targeted traceroute and BGP table dump is valid and these

peerings exist. Medium level confidence to those peering that has appeared at least in one of the approaches and low confidence to those which are available on the public projects datasets but none of the approach is able to detect them.

This did not reflect that low and medium confidence are poor results, it is just the fact that peering might exist but the approach used to detect them was might not sufficient or may be publicly available record was outdated. Success rate of finding an IXP and peering is very highly dependent on finding the Looking Glass Server in at least one member of the AS connected to the IXP. High confidence majority peering is on the left hand side of the graph because usually large IXPs have LG or Router servers available as compared to the small IXPs.

Figure 4: Peerings per IXP [12]

D. Reasons for Peering at IXPs?

The most conventional thought for creating a peering between two Internet Service Providers is to reduce the cost i.e. if the data traffic between two ISPs is exchanged through peering than there is no need to move that traffic towards a transit provider. Bypassing the transit provider advantages both ISPs to reduce their transit cost. This seems logically correct if two ISPs sharing high amount of traffic between each other and saving huge amount of money. It becomes critical if the two ISPs shares very low volume of traffic, then cost saving might not be the reason of peering because engaging in peering has some cost (maintenance, contracts and agreements, staff etc.).

One recent study [19] on a European based IXP Slovak (SIX) discusses this thing in more detailed and questioned that cost might not be the only factor influencing ISPs to peer with each other at IXPs. There are around 926 peering pairs in SIX. As shown in Fig. 5, estimated monthly traffic of SIX reveals the fact that out of those 926 peering links, approximately around 50% exchanges less than 1 Mbps of the traffic. An average estimation of IP transit in US and Europe is around 9-10 US dollars per Mbps per month but this pricing figure varies and depends a lot on geographical location and committed data rate as well. Still, peering links between ISPs which is having less than 1 Mbps traffic would result in very low cost reduction which might even lower than the maintenance and legal agreements which both ISPs has to pay to IXP. One observation is that cost is not the only factor for

peering at IXPs but sometimes performance factor is also considered. If the local traffic remains local and ISPs only use transit providers when there is a need of transit than this helps in better QoS as the number of hops the packet needs to traverse is reduced by peering.

Figure 5: Traffic Exchange between 926 Peering Pairs at SIX [19]

V. SUMMARY

IXPs play a vital role in the internet eco-level system mediating around 15-20% of internet inter-domain traffic. With the trend of bypassing the transit provider for cost reduction, the importance of peering at IXPs in general is like to increase. This paper study few approaches to map IXPs by various resources such as IXP databases; websites, IRR and looking for IXP related data in all the public places such CAIDA, DIMES. Also, we highlighted some techniques to find IXPs by using targeted traceroute LG servers and BGP tables. Such data not only allows us to characterize the AS level topology of the internet but also the dynamic properties of the IXPs. In this effort, we find that there is potentially 58k peering links and more than 200 IXPs operating around the world. By using these tools and the publicly available datasets will help in understanding the evolution of IXPs. It is also observed that once the member in an IXP peers with any other member, their peering is very likely to disappear unless one of the member disconnects from that IXP. By using state-of-the-art tools for measuring the bandwidth between those peering links in IXPs will be a challenging task but the way IXPs are growing in size, understanding these dynamic will have a huge impact for characterizing IXP related topology.

REFERENCES

- [1] M. Zubair and R. Guha, "Impact of Internet Exchange Points on Internet Topology Evolution", 35th IEEE Annual conference Local Computer Networks (LCN), 2010.
- [2] Y. He, G. Siganos, M. Faloutsos and S. Krishnamurthy, "Lord of the Links: a framework for discovering missing links in the internet topology", IEEE/ACM Transactions, Vol. 17, No.2, Pp 391-404, 2009.
- [3] R.V. Oliveira, W. Willinger, B. Zhang and L. Zhang, "In search of the elusive ground truth: The internet AS level connectivity structure", SIGMETRICS, Vol. 36, No.1, Pp 217-228, 2008.
- [4] H. Chang, R. Govindan, S. Jamin, S.J. Shenker and W. Willinger., Towards capturing representative AS-level Internet topologies. Computer Networks, Vol. 44, No. 6, Pp. 737-755, 2004.
- [5] L. Gao and J. Rexford, "Stable Internet Routing without Global Coordination", ACM SIGMETRICS, Vol. 28, No. 1, 2000.
- [6] CISCO, "The value of Peering", ISP/IXP Workshop, 2009.
- [7] C. Labovitz, S. Lelkel-Johnson and D. McPherson, "Internet Inter-domain Traffic", Proceedings of ACM SIGCOMM, 2010.
- [8] A. Dhamdhere and C. Dovrolis, "Ten years in the evolution of the internet ecosystem", Proceeding of ACM IMC, 2008.
- [9] H. Chang and W. Willinger "Difficulties measuring the Internet's AS level ecosystem", 40th conference, Information Sciences and Systems, 2006.
- [10] Z.M. Mao, J. Rexford, J. Wang and R.H. Katz, Towards an accurate AS-level traceroute tool. Conference on Applications, technologies, architectures, and protocols for computer communications, Pp. 365-378, 2003.
- [11] B. Augustin, B. Krishnamurthy and W. Willinger, "IXPs: mapped?", Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference, Pp. 336-349, 2009.
- [12] K. Xu, Z. Duan, Z.L. Zhang and J. Chandrashekar, "On properties of internet exchange points and their impact on as topology and relationship", Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications, Pp. 284-295.
- [13] Y. Shavitt and E. Shir, "DIMES: Let the Internet Measure Itself", CCR, Vol. 35, No. 5, Pp. 71-74, 2005.
- [14] J.C. Cardona Restrepo and R. Stanojevic, A history of an internet exchange point. ACM SIGCOMM Computer Communication Review, Vol. 42, No. 2, Pp. 58-64, 2012.
- [15] M. Marcon, M. Dischinger, K.P. Gummadi and A. Vahdat. "The Local and Global Effects of Traffic Shaping in the Internet", Proceedings of ACM SIGCOMM, 2008.
- [16] H. Chang, S. Jamin, Z. Mao and W. Willinger. "An empirical approach to modeling inter-AS traffic matrices", Proceedings IMC, 2005.
- [17] S. Akhshabi and C. Dovrolis, "The evolution of layered protocol stacks leads to an hourglass-shaped architecture", Proceedings of ACM SIGCOMM, 2011.
- [18] P. Borgnat, G. Dewaele, K. Fukuda, P. Abry and K. Cho, "Seven years and one day: Sketching the evolution of internet traffic", Proceedings of IEEE INFOCOM, 2009.
- [19] J.C. Cardona Restrepo and R. Stanojevic, A history of an internet exchange point. ACM SIGCOMM Computer Communication Review, Vol. 42, No. 2, Pp. 58-64, 2012.